coupled to network **110** via any operable link, such as example link **190**. Alternatively, a DMP appliance may provide a subset of DMP server and database functionality and/or may not be coupled to a network. Such an appliance may simply emit policy via RF means or acoustic means or the like.

[0017] FIG. **2** is a block diagram showing example mobile devices coupled to together via an ad-hoc network **210**. Such an ad-hoc network may not include any persistent devices such as DMP servers or related data stores. Ad-hoc networks for DMP purposes may be formed as various mobile devices form and join such networks. For example, an ad-hoc network may be formed comprising devices of people on a particular bus. Example devices shown in FIG. **2** include those described in connection with FIG. **1**.

[0018] FIG. **3** is a block diagram showing an example device manners policy ("DMP") **310** applied to an example mobile device **180** as indicated by arrow **330**. Such a DMP may originate from a DMP server, such as server **120** and related data store **122**, and may be transferred or downloaded **320** to a device such as mobile device **180**. Alternatively, DMP **310** may be created on device **180** or transferred to device **180** via other means.

[0019] Upon receipt of DMP **310** by device **180**, DMP **310** may be evaluate to determine what, if any, compliance may be suggested or required. In one example, a DMP may be received by cell phone **180** upon entering a hospital, the DMP requiring no cell phone usage. Cell phone **180** may be operable to comply with such a DMP by shutting down, entering a sleep mode, or the like. Upon leaving the hospital cell phone **180** typically returns to its previous mode of operation as the hospital DMP is no longer applicable.

[0020] In another example, service provider **350** may require that a device provide an indication of DMP compliance capability prior to or for continuation of services, such as over link **352**. Device **180** may provide such an indication **360** to service provider **350** to satisfy the requirement. Further, service provider **350** may transfer various DMPs to device **180** in connection with the services provided. For example, a museum may include service provider **350** to provide wireless data access to various devices though which information about the exhibits may be accessed. Provider **350** may further propagate a DMP indicating "no photography". Devices receiving such DMP upon entry to the museum typically initiate compliance with the "no photography" DMP by disabling any photography capabilities, such as provided by cell phone cameras, digital cameras, and digital video recorders. Access to exhibit data may be subject to indication of compliance.

[0021] In yet another example, the "no photography" DMP may be provided in the form of a special tag such as a unique watermark (generally not visible to humans), radio frequency identification ("RFID") device, or the like located on or near various exhibits, such a tag being detectable and/or identifiable by a DMP-enabled device via optical, RF, or other appropriate means. In this example a network, ad-hoc or otherwise, may not be required for at least some forms of DMP compliance.

[0022] In yet another example, a "no recording" DMP may be provided in the form of an audio signal, typically inaudible to human listeners, in connection with music or some other audio or audio/video reproduction. Such an audio signal may be detected and identified by a DMP-enabled device such as a digital recorder, a digital video recorder, or the like. In this example a network, ad-hoc or otherwise, may not be required for at least some forms of DMP compliance.

[0023] In yet another example, a "no noise" or "no light" DMP may be provided via a network, audio means, or any other suitable means or combination of means, the DMP being detectable and/or identifiable by a DMP-enabled device such as a device that may emit light or sound including, but not limited to, watches with audible alarms, shoes with lights (as sometimes worn by children, for example), cameras, flashlights, cell phones, PDAs, or any other device that may benefit from compliance with a "no noise" or "no light" DMP or the like.

[0024] In yet further examples, DMPs may be used in particular zones to limit the speed and/or acceleration of vehicles, to require the use of lights, to verify an indication of insurance coverage and/or current registration, or the like. DMPs may be propagated with acceptable usage times for mobile devices, such as when on an airplane with being restrictions common at times of landing and/or take-off. DMPs may be used to cause devices to be reconfigured for silent operation in locations such as libraries, court rooms, hospitals, meeting rooms, theatres, or the like.

[0025] In ad-hoc scenarios, DMPs may be the result of voting or a consensus among current members of an ad-hoc network or the like. For example, the majority of current bus riders may agree upon and propagate "silence please" DMPs that cause cell phones to reconfigure for vibrate versus audible rings, that cause audio devices to work only with headphones, that cause gaming devise to switch to a silent mode of operation, and the like.

[0026] In general, DMPs may be applied to devices when within a particular zone or area to which the DMPs apply. Upon leaving such zones or areas a device is typically reconfigured to resume it former mode of operation. For example, a cell phone device reconfigured to a vibrate mode as a result of detecting a "silence" DMP upon hospital entry will typically return to its previous ring mode when leaving the hospital zone. In other scenarios, a device may revert back to a previous configuration when leaving a virtual community such as may be established via an ad-hoc network. Such DMP zones, areas, communities, or the like may be defined and/or indicated in any manner useful for DMP propagation and compliance purposes.

[0027] DMP **310** typically includes one or more device manners ("DM") that specify particular device behaviors or rules to which device compliance is requested or expected. Typically it is the responsibility of the device itself to comply with any applicable DMs in a recognized DMP, as well as determining applicability. Device compliance is generally achieved via self-reconfiguration. Restoration of a device's previous configuration typically occurs when a DMP is no longer applicable, such as when the device is no longer in the DMP's zone, area, community, or the like. Additionally or alternatively, a DMP may include an expiration time, a timeout period, or the like, upon which a device in compliance with such a DMP may revert back to a previous configuration. Further, a DMP may require that a hosting device report its compliance status back to the source of the DMP such that non-compliant devices, or the compliance status of devices, may be noted by a DMP environment.

[0028] DMP **310** may be implemented as a data structure, an electronic signal, represented via extensible markup language ("XML") or the like, expressed as an image, or otherwise implemented, expressed, and/or represented sufficient